255 Fiserv Drive
Brookfield, WI 53045
www.fiserv.com

fiserv.

January 11, 2017

VIA ELECTRONIC MAIL

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW.
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th St. SW
Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

Robert E. Feldman, Executive Summary
Federal Deposit Insurance Corporation
550 17th St. NW
Washington, DC 20429

Re: ***Advance Notice of Proposed Rulemaking - Enhanced Cyber Risk Management Standards, Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45***

Dear Ladies and Gentlemen:

This letter includes comments on the Advance Notice of Proposed Rulemaking ("ANPR") referenced above on behalf of **Fiserv, Inc.** ("Fiserv") and its subsidiaries.

Fiserv (NASDAQ: FISV) is a FORTUNE 500 company and has been a global leader in financial services technology for more than 30 years, enabling clients to achieve best-in-class results by driving quality and innovation in payments, processing services, risk and compliance, customer and channel management, and business insights and optimization. Fiserv subsidiaries render services to financial institutions that would be deemed "covered entities" potentially subject to the standards described in the ANPR. Some of those services may also be deemed "covered services" under the ANPR to which the Agencies are considering application of the standards.

Fiserv is commenting on Questions 4, 5, 6, 11, 21, 22, 24, 29, 30, 31, 32, and 37.

Question 4. What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to

maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?

The Gramm Leach Bliley Act Safeguards Rule applies directly to financial institutions (not service providers) and includes a requirement that financial institutions bind their service providers by contract to certain obligations, and holds them accountable to manage and monitor their service providers. Fiserv believes that this approach is familiar and well understood by financial institutions, regulators, and the public, has been effective in establishing an industry cybersecurity standard that achieves cybersecurity protection while preserving performance, and should be adopted pursuant to the ANPR.

This indirect approach to subjecting covered services to enhanced standards has several significant advantages in comparison to the direct approach being considered by the agencies according to the ANPR: (1) lower likelihood of conflict between covered entities and their service providers over implementation of the standards due to covered entities' and service providers' differing interpretations of the standards or inconsistent direction from different regulatory examiners who are tasked with interpreting the standards; and (2) greater efficiency and effectiveness in risk mitigation resulting from financial institutions and their service providers being able to negotiate security controls that are consistent with the parties' existing security programs and particular set of risks.

The approach of applying standards to the financial institutions and requiring them to bind their service providers accordingly empowers and appropriately incents each financial institution to manage its service providers carefully, and does not risk lessening the cyber risk management standards that apply to covered services to the extent that, as could be the case under a direct approach, such standards are interpreted based only on the service provider's discretion and not in the context of an institution's third-party risk management program.

A disadvantage of the indirect approach from the perspective of the covered entity is that it requires covered entities to conduct due diligence and exercise oversight with respect to their service providers rather than relying on examinations of the service provider by a regulator. However, the agencies have devoted significant resources recently to third-party risk management – in the form of new third-party risk management guidance (e.g., Federal Reserve SR Letter 13-19, OCC Bulletin 2013-29, FDIC FIL-44-2008) and through supervisory tools such as the FFIEC Cybersecurity Assessment Tool – that have helped to facilitate and enhance the due diligence and oversight that covered entities are to conduct of service providers. The indirect approach remains the predominant model for service provider regulation today because it appropriately encourages financial institutions to remain diligent in their monitoring of service providers and leverages the robust third-party risk management programs institutions have established pursuant to existing regulatory guidance.

Question 5. What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?

Direct application of the enhanced cyber risk management standards to service providers would have the advantage of enabling covered entities to rely, to some extent, on the findings of service provider examinations conducted by the agencies, recognizing that the opportunity for this reliance already exists today to the extent a service provider, such as Fiserv, is examined directly by a regulator. At the same time, wholesale reliance on such an examination is inconsistent with the third-party risk management principles articulated by the agencies that require an institution to conduct its own due diligence and exercise oversight and therefore is of uncertain practical value to an institution.

Disadvantages of direct application of the enhanced standards to service providers, as described above, include: (1) lower likelihood of conflict between covered entities and their service providers over implementation of the standards due to covered entities' and service providers' differing interpretations of the standards or inconsistent direction from different regulatory examiners who are tasked with interpreting the standards; and (2) greater efficiency and effectiveness in risk mitigation resulting from financial institutions and their service providers being able to negotiate security controls that are consistent with the parties' existing security programs and particular set of risks.

As a general matter, applying rules directly to the service provider – and examining the service provider's interpretation and implementation of those rules – very well could generate industry conflict and friction, rather than much-needed alignment and collaboration, between financial institutions and their third party service providers on the critical topic of cybersecurity.

Question 6. What factors are most important in determining an appropriate balance between protecting the safety and soundness of the financial sector through the possible application of the standards and the implementation burden and costs associated with implementing the standards?

Fiserv considers the following factors to be critical in determining the balance between safety and soundness and the burdens of implementation:

(1) Standards should not dictate specific security controls but rather require a process in which risks are assessed and appropriate controls are implemented to address the identified risks. First, the range of services provided to financial institutions and their clients is too broad to apply specific security controls across the board to each and every service. Second, information security technology evolves rapidly, often outpacing updates and revisions to such standards by the agencies. As a result, if specific security controls are prescribed in an information security standard, companies may be forced to choose between being in compliance with the standard but using outdated technology or using new technology but being out of compliance with the standard.

(2) There should be flexibility in the selection of specific controls to satisfy the standards so that there is competition among service providers in terms of innovation and pricing in order to further enhance cybersecurity protections. The service provider community can serve as a laboratory for cybersecurity solutions that contributes to enhanced security and stability over time.

(3) Security goals can and should be commercially reasonable (e.g., a commercially reasonable level of residual risk should be permitted even after controls are in place, recognizing that zero risk is not attainable at any price, and that controls should not cost more than the potential foreseeable loss).

Question 21. How would the proposed standards for internal and external dependency management impact a covered entity's use of a third-party service provider?

The term "external dependency" in the ANPR refers to an entity's relationships with outside vendors, suppliers, customers, utilities (such as power and telecommunications), and other external organizations and service providers that the covered entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties. The agencies are considering a requirement that covered entities analyze and address the cyber risks that emerge from reviews of their external relationships, and identify and periodically test alternative solutions in case an external partner fails to perform as expected. As part of this requirement and in order to address the rapidly changing and complex threat landscape, the agencies are considering a requirement that covered entities continually apply and evaluate appropriate controls to reduce the cyber risk of external dependencies to the enterprise and the sector.

These proposed requirements could, if drafted and implemented in an overly rigid fashion, impose undue costs and burdens on the outsourcing of processing and other services to third-party service providers, which already are subjected to robust internal controls. Under current practice, large financial institutions typically require completion of a security questionnaire at the outset of the relationship and annually thereafter, and retain a contractual right to audit their service providers annually or in the event of an incident in which data of the financial institution or its customers is disclosed or accessed in an unauthorized manner. Contracts also frequently require reports of penetration testing of applications (upon initial coding and when major code changes are made), and testing of externally facing infrastructure (annually for penetration tests and quarterly for vulnerability scans). More frequent or extensive monitoring and auditing could become unduly costly and burdensome, particularly for service providers that provide services to significant numbers of covered entities.

Question 22. What additional issues should the agencies consider related to internal and external dependency management and the covered entities' use of third-party service providers? How should those issues be evaluated by the agencies? Please be specific.

The agencies should consider the impact of shared infrastructure on enhanced cyber risk standards. For example, in order to promote efficiencies, stability and effective performance, service providers commonly provide services to financial institution clients, including larger institutions, on shared (multi-tenanted) platforms, servicing multiple clients through separate and secure "instances" of the platform. Each client may not have its own dedicated or separate servers or databases. Confidential information is logically separated rather than physically separated. Therefore, common processes and controls are used for multiple clients on these platforms rather than unique processes and controls for each client. As a result of delivering services from infrastructure that is shared among a set of clients, service providers may need to summarize reports or redact them to protect the confidentiality of other clients, and control and monitor audits and testing to protect the confidentiality of other clients. Security standards and dependency management should accommodate shared infrastructure and not require each client (or their designated third-party) to obtain dedicated or unrestricted access to, monitoring of, and reporting from, service provider systems. Security standards should also not assume that clients will be

allowed to load their own software or customized software on the service provider's system, install their own appliances or customized appliances or other hardware on the service provider's network, or demand architectural changes to the service provider's infrastructure.

Question 24. What is the extent to which it would be operationally and/or commercially feasible to comply with requirements to use certain defined data standards in order to increase the substitutability of third-party relationships to reduce recovery times for systems impacted by a significant cyber event?

The agencies are considering whether to require covered entities to establish protocols for secure, immutable, off-line storage of critical records, including financial records of the institution, loan data, asset management account information, and daily deposit account records (e.g., balances and ownership details), all formatted using certain defined data standards to allow for restoration of these records by another financial institution, service provider, or the FDIC in the event of resolution. This type of data is currently stored and processed in a variety of platforms written in and supported by various technologies and in a variety of formats, so enforcing "defined data standards" will impose substantial challenges and costs. Accordingly, we do not view the adoption of defined data standards as the optimal operational or commercial approach to reducing recovery time in the event of an incident. Among other things, re-engineering systems and processes so as to continually load and update data in "off-line storage" for subsequent retrieval (along with periodic testing of the backup and retrieval processes) will impose substantial challenges and costs and could also slow transactional response times. Management of encryption keys to allow retrieval of encrypted information by other parties will also present challenges.

However, there are initiatives underway that may address concerns about information security recovery without the need for the imposition of additional data standards. For example, Fiserv has been participating in "Sheltered Harbor" discussions guided by the Financial Services Information Sharing and Analysis Center (FS-ISAC). Sheltered Harbor is a voluntary effort to create the capability to preserve a narrow set of critical records in case of a cyber event. Standards for data formats, offline storage, and the transfer of records have been formulated for retail banking and brokerage accounts, and are being implemented by financial institutions and service providers. The industry fully expects to implement standards for additional asset classes as the effort progresses. Doing so for a very narrow, defined set of data fields applicable to specific financial sectors or kinds of accounts is possible, but establishing standards broadly across many data sets or multiple industries would be very challenging and costly. It is generally agreed that a recovery pursuant to the Sheltered Harbor would only apply after all other Business Continuity Planning (BCP) efforts have failed. This has implications for the timing of when it would be possible to effect a complete "return to operations." (See the response to question 29 for further information.) Restoration time expectations continue to be analyzed by FS-ISAC for situations in which a decision is made to transfer business operations to another entity or service provider, and are expected to be measured in days, due to the current magnitude of technical, business and regulatory challenges.

Question 29. The agencies request comment on the appropriateness and feasibility of establishing a two-hour RTO for all sector-critical systems. What would be the incremental costs to covered entities of moving toward a two-hour RTO objective for these systems?

The agencies are considering requiring covered entities to establish a Recovery Time Objective (RTO) of two hours for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive, or destructive cyber event. As defined in the ANPR, an RTO is the "amount of time in which a firm aims to recover clearing

and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date." The scope of application of this proposed sector-critical standard could go beyond core clearing and settlement organizations to include other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector.

To assess this proposal in a meaningful way, the agencies should provide additional information, including further detail on the systems that would be in scope, the kinds of cyber events contemplated, the Recovery Point Objectives that would apply, tolerable levels of data loss, and the types of data validations (potentially including multiple transmissions) that would be required to protect against data loss. A two-hour RTO would require network switching from financial institutions to alternative locations to be identified in advance and periodically tested. In any event, a two-hour RTO across all systems would likely be a substantial and costly undertaking, and for some systems may not be feasible.

As discussed in our response to Question #24 above, Fiserv has been participating in "Sheltered Harbor" discussions guided by FS-ISAC. It is generally agreed that a Sheltered Harbor recovery only applies after all other BCP efforts have failed. This implies that a "return to operations" as contemplated by the RTO standard may not be easily undertaken in the event of a catastrophic cyber event. As described above, restoration time expectations continue to be analyzed for situations in which a decision is made to transfer business operations to another entity or service provider, and are reasonably expected to be measured in days, due to the current magnitude of technical, business and regulatory challenges.

Question 30. What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How should the agencies weigh such costs against other costs associated with implementing the enhanced standards outlined in this ANPR?

Covered entities under the ANPR use third-party service providers for a wide variety of services. A two-hour RTO for critical systems of covered entities would almost certainly require substantial system upgrades and process improvements by third-party service providers as well as upgraded integration and coordination between covered entities and service providers, the costs of which would be, at least in substantial part, incurred by or passed through to the covered entities and ultimately to consumers. The agencies should give substantial weight to the initial and ongoing costs of these upgrades, and at the very least allow for a feasible amount of time to implement any such upgrades.

Challenges presented by the requirement of a two-hour RTO would include not only replicating the real time transactions in that time frame, but also the recovery of scheduled batch processes and file transmissions, and in-flight processes. Validation of the various processing states of each system in order to restart each one will also be challenging, unless all support functions and databases and individual files are also replicated in real time.

Question 31. How should the agencies implement the two-hour RTO objective? For example, would an extended implementation timeline help to mitigate costs, and if so, what timeline would be reasonable?

To meaningfully assess this proposal, the agencies should provide additional information identifying the systems that would be subject to the objective and the types of cyber events contemplated. In any case, establishing a two-hour RTO for all such systems and scenarios would likely be a substantial and costly undertaking and may not be feasible for some systems. Bringing the substantial majority of systems into compliance with this objective would require a multi-year project and substantial information security expenditures.

Question 32. Should different RTOs be set for different types of operations and, if so, how? Should RTOs be expected to become more stringent over time as technology advances?

To the extent the agencies implement an RTO standard, different RTOs should be set for different types of operations or different types of cyber threats. For example, an RTO for operations in which batch processes are involved should be longer than operations in which only real time transactions are involved. Longer RTOs would likely be needed when there are significant system dependencies, as is frequently the case when financial institutions use databases or files from multiple systems. In theory, RTOs may be expected to become shorter in duration over time as technology evolves, but this does not take into account the rise in sophistication of security threats. All in all, the evolution in technology cannot reliably be predicted with sufficient certainty to justify a standard that declines automatically over time. Any modifications to RTOs need to be based on industry feedback following notice and comment rulemaking.

Question 37. What are the potential benefits or drawbacks associated with each of the options for implementing the standards discussed above?

The agencies are considering three options for implementing the standards:

(1) the agencies could (similar to the way the Gramm Leach Bliley Act and implementing guidance functions) propose the standards as a combination of a regulatory requirement to maintain a risk management framework for cyber risks along with a policy statement or guidance that describes minimum expectations for the framework, such as policies, procedures, and practices commensurate with the inherent cyber risk level of the covered entity;

(2) the agencies could propose regulations that impose specific cyber risk management standards in the five categories of cyber risk management in the ANPR, and require covered entities to establish and maintain policies, procedures, practices, controls, personnel and systems that address each applicable category, and to establish and maintain a corporate governance structure that implements the cyber risk management program on an enterprise-wide basis and along business line levels, monitors compliance with the program, and adjusts corporate practices to address the changes in risk presented by the firm's operations; and/or

(3) the agencies could propose a regulatory framework that is more detailed than the second approach, including details on the specific objectives and practices a firm would be required to achieve in each area of concern in order to demonstrate that its cyber risk management program can adapt to changes in a firm's operations and to the evolving cyber environment.

In considering which option, or combination of options, to adopt, the agencies should consider (i) whether the approach ensures that the enhanced standards are clear, (ii) the additional effort and cost required to implement the standards, (iii) whether the standards are sufficiently adaptable to address the changing cyber risk environment, and (iv) the potential costs and other burdens on covered entities, service providers and consumers that could result from such standards. Applying these considerations, Fiserv believes that the first option should be adopted – *i.e.*, implementation of a combination of a regulatory requirement to maintain a risk management framework for cyber risks along with guidance that describes minimum expectations for the framework, such as policies, procedures, and practices commensurate with the inherent cyber risk level of the covered entity. This approach has the advantages of being similar to the Gramm Leach Bliley Act framework with which financial institutions and their service providers are already familiar, and providing sufficient flexibility for each covered entity to design and implement a cybersecurity program that addresses its own set of risks and to negotiate supporting cybersecurity measures with its service providers as applicable and tailored to the nature, type, quantity and criticality of the specific services performed by the service provider.

The second and third options are too prescriptive and would likely impose unnecessary effort and costs on covered entities and their service providers.

Fiserv would like to thank the agencies for taking a carefully considered approach to this important and complex subject, and for inviting and considering comments from the industry.

Sincerely,

Lynn S. McCreary
Chief Legal Officer
Fiserv, Inc.